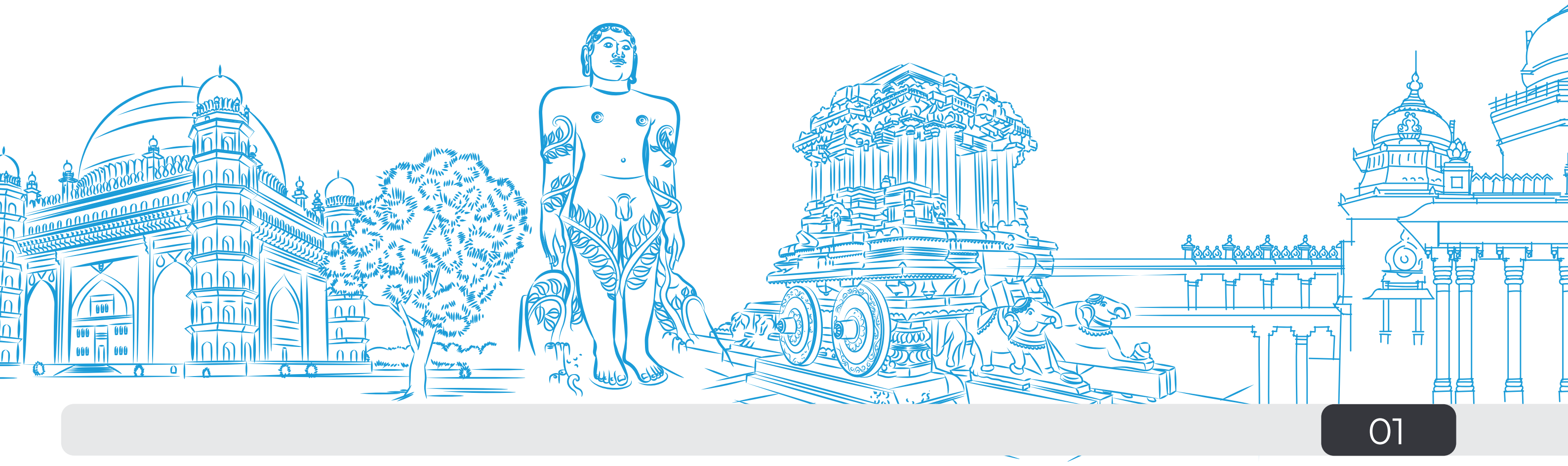
GOVERNMENT OF KARNATAKA

KARNATAKA CYBER SECURITY POLICY 2024

Shri Siddaramaiah
Hon’ble **Chief Minister**
Government of Karnataka

I am pleased to introduce our New Cyber Security Policy 2024, a crucial step towards keeping our state safe in the digital world. We live in a time where our daily lives, work, and government services are online. With this comes the risk of cyberattacks, which we are determined to fight with this new policy. Karnataka is known for its leadership in technology, and we want to make sure that our digital space is safe for everyone. This policy is not just about using the latest technology to protect us. It's also about making sure that people know how to be safe online, training experts to defend against attacks, and working together with businesses and other experts to make our defenses even stronger. I am proud to announce this policy and I extend my gratitude to all stakeholders who have participated in the process of drafting this Policy.



Shri Priyank M Kharge

Hon’ble Minister for IT, BT, and Rural
Development and Panchayat Raj
Government of Karnataka

In the era of digital transformation, cybersecurity has become a cornerstone for safeguarding the integrity, confidentiality, and availability of information. The Government of Karnataka, recognizing the criticality of this domain, has meticulously crafted the Cyber Security Policy to establish a resilient and secure cyberspace for our citizens and enterprises.

The policy, aligned with national and international efforts, underscores our state's proactive stance in combating cyber threats. It is structured around five strategic pillars: Building Awareness, Skill Building, Promoting Research and Innovation, Promotion of Industry and Start-ups, and Partnerships and Collaborations for Capacity Building. These pillars are designed to foster a culture of cybersecurity that permeates every level of our digital ecosystem.

Karnataka's commitment to cybersecurity is evident in our initiatives such as the establishment of a Cyber Security Centre of Excellence and the promotion of cybersecurity awareness among the public. We are also dedicated to enhancing the skills of our workforce to meet the growing demand for cybersecurity professionals.

As the Minister of the Government of Karnataka, I am confident that the implementation of this policy will significantly contribute to the protection of our digital infrastructure. It will also encourage innovation and growth within the cybersecurity sector, ensuring that Karnataka remains at the forefront of technological advancement.

I commend the collaborative efforts of all stakeholders involved in the development of this policy and urge its rigorous implementation. Together, we will achieve a secure and prosperous digital future for Karnataka.

Table of CONTENTS

PREAMBLE

Karnataka is a leading state in India in the promotion of IT and emerging technologies. In addition to being the largest IT hub in the country that has directly and indirectly provided employment to several millions and catalysed transformative innovations, Karnataka has also instituted several landmark e-Governance initiatives for seamless delivery of services to the public. The government has been a key driver for increased adoption of IT-based products and IT enabled services in Public services (Government to citizen services, GramaOne Centers, SevaSindhu, Family ID, SSP, FRUITS, public distribution systems etc), Healthcare (telemedicine, remote consultation, mobile clinics), Education (e-Learning, virtual classrooms, etc) and Financial services (DBT, Khajane 2.0, mobile banking / payment gateways), etc. Such initiatives have enabled increased IT adoption in the state through sectoral reforms and National & State programmes which have led to creation of large-scale IT infrastructure with corporate / private participation.

In the light of the growth of IT sector in the State, ambitious plans for rapid social transformation leveraging Information Technology, and Karnataka State's prominent role in the global IT market, providing right kind of focus for creating secure computing environment and adequate trust & confidence in electronic transactions, software, services, devices and networks has become one of the compelling priorities for the State. Such a focus enables creation of a suitable cyber security eco-system and establishes cyber strategy for the State, in tune with national interest and globally networked environment.

Cyberspace is a complex environment consisting of interactions between people, software and services, supported by worldwide distribution of information and communication technologies (ICT) devices and networks. Owing to the numerous benefits brought about by technological advancements, the cyberspace today is a common pool used by citizens, businesses, critical information infrastructure, military and governments in a manner that makes it difficult to draw clear boundaries among these different groups. The cyberspace is expected to be more complex in the foreseeable future, with many folds increase in networks and devices connected to it.

There is now hence a need for these actions to be unified under a Cyber Security Policy that will be in line with National Cyber Security Policy, with an integrated vision and a set of sustained & coordinated strategies for implementation. This Cyber Security Policy hence comprises of both the policy for the state's IT teams, as well as the strategy the state will adopt to develop a strong cyber security ecosystem.

This policy has been drafted jointly by the Department of Electronics, IT, Bt and S&T, Department of Personnel and Administrative Reforms (e-Governance) and Home Department, in consultation with all the relevant stakeholders.

The first part of the Cyber Security Policy will be in public domain and addresses the issues of awareness, skill-building and promotion of innovation, industry and start-ups. The rapid adoption of IT by citizens, industry and government has enhanced quality of life, enabled significant productivity gains and improved efficiency and effectiveness of service delivery. The COVID-19 pandemic has accelerated the digitisation of business, processes, operations and financial interactions worldwide, often without adequate planning and safety measures. Also, due to the rapidly evolving nature of technology, the inherent connectedness of cyberspace and the anonymity it offers, today the risks of falling prey to cyber-crimes is increasing with increasing adoption of technology.

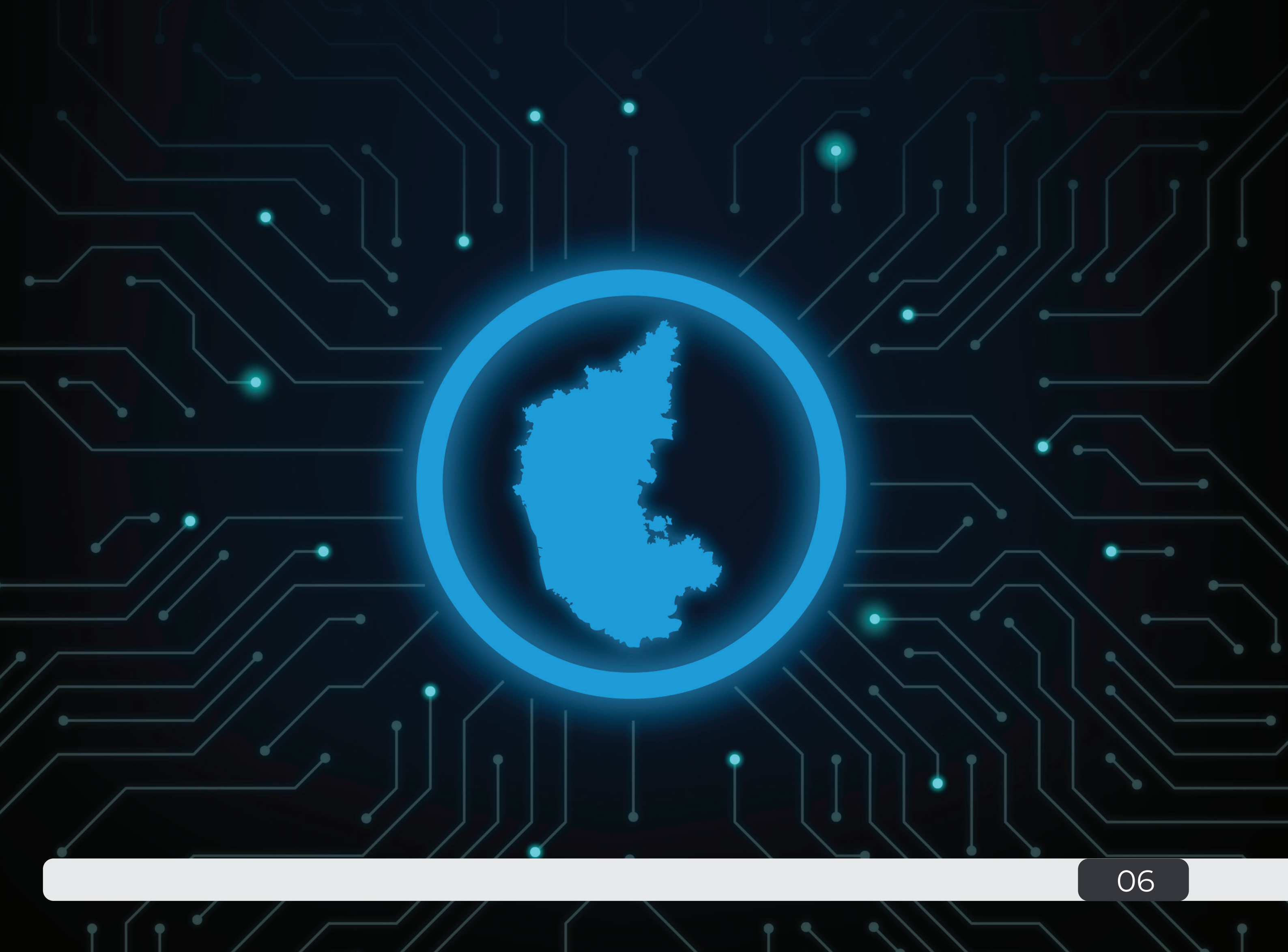
The second part of the policy will be internal to the state's IT teams and departments for their IT implementations, and complements the first part by focusing on strengthening the cyber security posture of the State's IT assets. It aims to build a dynamic, secure and resilient cyberspace for all the G2G, G2B and G2C services of Government of Karnataka. It serves as an umbrella framework for defining and guiding the actions related to security of the state's IT systems. It also enables the individual sectors and organizations in designing appropriate cyber security policies to suit their needs. The policy provides an overview of what it takes to effectively protect information, information systems & networks, and also gives an insight into the Government's approach to enable collaborative working with all key players in public & private sectors to safeguard state's information and information systems.

Cyber security failure is emerging to be one of the most devastating and likely set of risks to be tackled globally. India was subject to the third highest number of significant cyber-attacks in the period between 2006-2020. Cyber threats – including script kiddies, hacktivists, crime syndicates and nation-state actors – pose a significant challenge to the goal of enabling citizens to "go digital". Further, as citizens operate in cyber space, their right to privacy needs to be protected as recognised by the Supreme Court of India. Adolescents and other vulnerable sections of society also suffer online harm. Further, the exponential increase in the amount of data generated and shared online, results in increasing risk to privacy.

Digital India needs a strong foundation of cyber security, cyber safety and privacy. Karnataka, as a leader in Information Technology, is ideally poised to be a leader in this triad of cyber security, safety and privacy and build a strong cyber security ecosystem. This policy, therefore, aims to create a cyber security framework, which leads to specific actions and programmes to enhance the security posture of the State's cyber space.

VISION

> “To make Karnataka the leading cyber security hub in the country by instilling a culture of cyber security and data privacy amongst citizens and businesses, and promoting a thriving cyber security industry and start-up ecosystem in the state.”



International Efforts

The global nature of risks in cyberspace and interconnectedness of devices, networks and people in this field has necessitated collaborative international efforts in securing cyberspace. However, this has resulted in a fragmented regulatory landscape.

An early effort was made by the International Telecommunication Union (ITU), a specialised agency of the United Nations (UN), which launched the Global Cyber Security Agenda in 2007 as a framework for international cooperation in this area. More recently, the Secretary-General of the UN established a Group of Governmental Experts on advancing responsible state behaviour in cyberspace (GGE), which consists of 25 countries including India, which is due to submit its final report to the General Assembly this year.

Apart from efforts at the nation state level, coalitions of stakeholders including industry and governments, have driven various efforts in this space. For example, the Paris Call for Trust and Security in Cyberspace led by the French government in 2018 is a nonbinding declaration that calls for states, the private sector, and civil society organizations to work together to promote security in cyberspace, counter disinformation, and address new threats endangering citizens and infrastructure. Similarly, some global industry wide consortiums have adopted self-regulatory norms. For example, the Microsoft driven Cybersecurity Tech Accord is a public commitment among more than 80 global companies to protect and empower civilians online and to improve their security. Charter of Trust, initiated by Siemens, calls for binding rules and standards to build trust in cyberspace and for the protection of data of individuals and businesses.

In parallel, various regional international collaborative efforts in this space are evolving. The African Union has published the Draft African Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa. The European Union (EU) has recently published a Joint Communication on the Cyber Security Strategy of the European Union, which is the first attempt for a comprehensive EU policy document in this domain to reflect the common view on cyber security of all its 27 member states. The NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) is a North Atlantic Treaty Organization (NATO) accredited organization that focuses on a range of aspects related to cyber security, such as education, analyses, consultation, lessons learned, research and development.

India is part of the Asia Pacific Computer Emergency Response Team (APCERT) involving leading national Computer Security Incident Response Teams (CSIRTs) from the economies of the Asia Pacific region to improve cooperation, response and information sharing among CSIRTs in the region. India regularly participates in drills and exercises conducted by APCERT.

National Efforts

According to the Global Cybersecurity Index 2020 by the ITU, India ranks as the 10th best country in the world on key cyber safety parameters assessed along five pillars – (i) Legal Measures, (ii) Technical Measures, (iii) Organizational Measures, (iv) Capacity Development, and (v) Cooperation. This is due to the various efforts made towards securing cyberspace through national and state efforts.

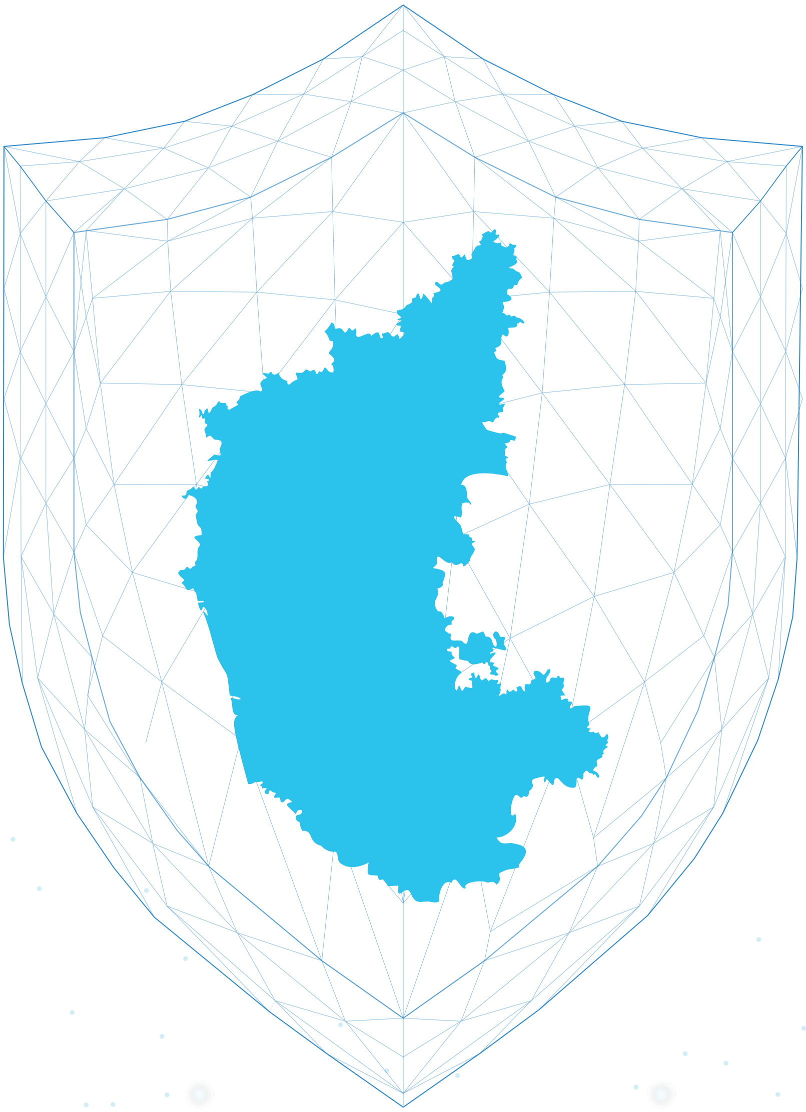
The National Cyber Security Policy (2013) is a national level framework that provides high level objectives and broad strategies for strengthening India's cyber security framework, improving e-Governance structures and services, capacity building, and the protection of Critical Information Infrastructures (CIIs). There are also sectoral regulations dealing with cyber security, such as the National Information Security Policy (2014), the SEBI Circular on Cyber Security and Cyber Resilience of Stock Exchanges, the RBI Cyber Security Framework for Banking, and the Guidelines on Information Security for Insurers (2017). The National Critical Information Infrastructure Protection Centre (NCIIPC) was formed under Section 70A of the IT Act, and has released revised guidelines in 2015, specifying five levels of control for CIIs in the country. The National Cyber Coordination Centre (NCCC) was set up to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive, and protective actions by individual entities. Phase-I of NCCC has been made operational.

In addition, the Information Technology (Computer Emergency Response Team) Rules, 2013 have been enacted under Section 70B of the Information Technology Act, 2000, pursuant to which the CERT-In has been operational since the enactment. The above-mentioned Rules require private entities affected by data breaches to promptly report such incidents to CERT-In.

State Efforts

Certain states have also adopted cyber security policies. These policies provide broad objectives and establish specialised agencies in the states to coordinate between various governmental agencies which are handling information assets, as well as private agencies which may be entrusted with government projects. The state policies provide for the formation of a security infrastructure, a computer emergency response team, and a Cyber Crisis Management Plan for the state.

In Karnataka, the Karnataka Jnana Aayoga set up a Task Group comprising eminent experts from the government, industry and academia that prepared a Cyber Security Vision 2025 report in 2019. The Karnataka Information Technology Policy 2020-2025 identified the need for the state to evolve a Cyber Security Policy, which was followed by a budget announcement in 2021-22.



DEFINITIONS

Term	Definition
Amicus	An impartial adviser to a court of law in a particular case
Catfishers	An individual who uses the Internet assuming a false identity to develop relationships for financial gain.
Critical Information Infrastructure	Those computer resources, the incapacitation or destruction of which, shall have debilitating impact on national security, economy, public health or safety.
Cyber Crisis Management Plan	A strategic framework for effective cyber security incident detection, incident management and incident response.
Cyber hygiene	Best practices to be followed in using the internet for cyber safety and prevention of being subject to cyber frauds.
Cyber range	A platform that provides hands-on cybersecurity practice to teams of professionals.
Cyber security	The protection of computer resources and networks from unauthorised access, information disclosure, theft of data or disruption of activities conducted on the computer resource or network.
Cyber security audit	A periodic and comprehensive review and analysis of the IT infrastructure of an entity to identify vulnerabilities in relation to cyber security.
Cyber security standards	Techniques, best practices and/or certifications adopted to protection IT infrastructure from cyber threads. Cyber security standards are often adopted on a large scale to bring uniformity to industry on a national or global level.
Data Privacy	The relationship between collection and dissemination of data (which may be personal or non-personal) and expectations of confidentiality and privacy of those providing the data.
Digital Literacy	Development of necessary skills for communication and accessing information in cyberspace and communicating with others
Hacktivists	A person who gains unauthorized access to computer files or networks in order to further social or political ends
Metadata	A set of data that describes and gives information about other data but not the content of the data.

DEFINITIONS

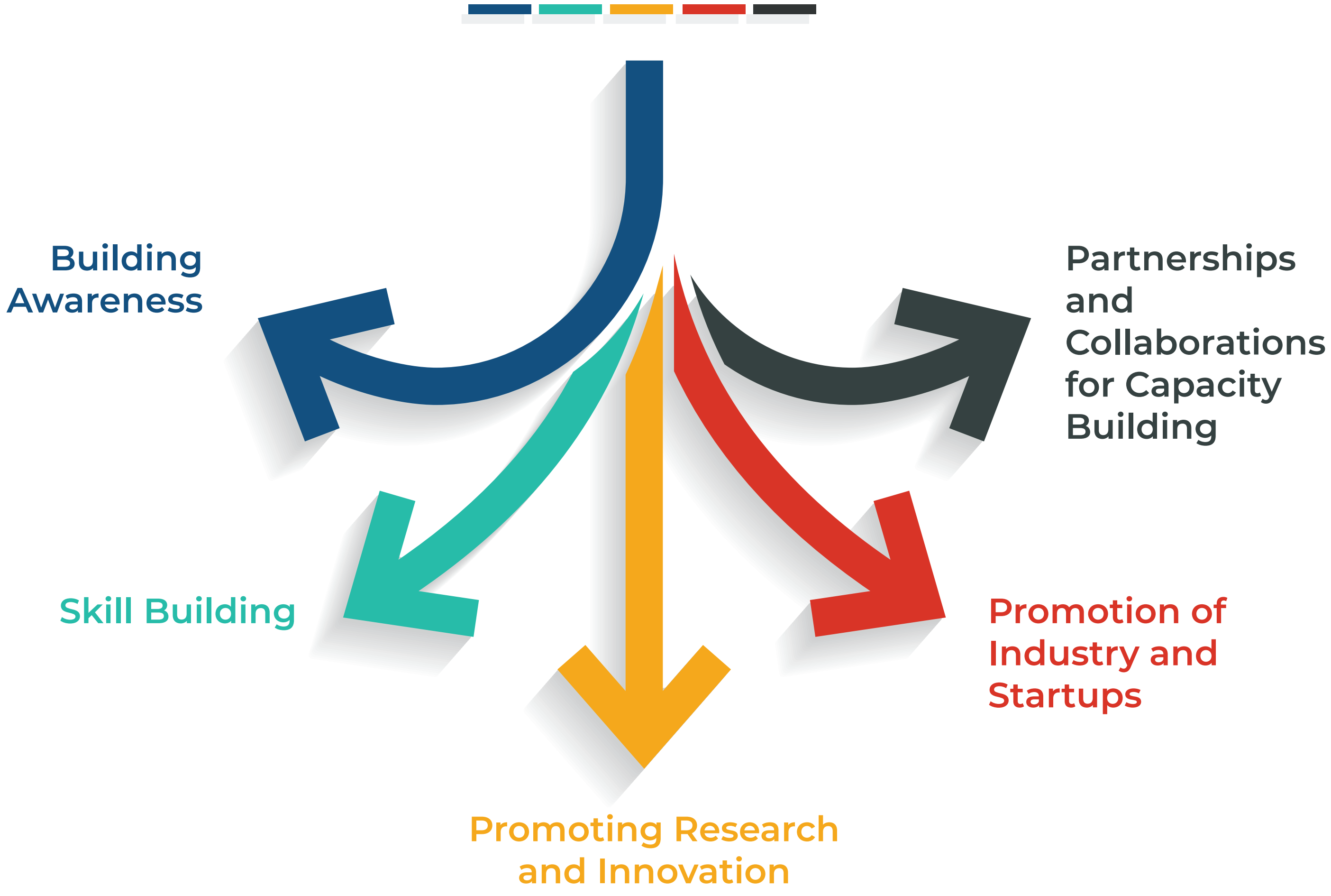
Term	Definition
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
Privacy and Security by Design	An approach to engineering and development calling for privacy to be taken into account throughout the whole product development and innovation process, to ensure foundational security.
Script kiddies	A relatively unskilled individual who uses scripts or programs, such as a web shell, developed by others to attack computer systems and networks and deface websites.

POLICY STRATEGY

This Cyber Security Strategy focuses on five main pillars, representative of the main stakeholders of the cyber security ecosystem – citizens of the state, technology professionals, researchers, industry, and the government. These are:

1. Building awareness
2. Skill building
3. Promoting research and innovation
4. Promotion of Industry and Start-ups
5. Partnerships and Collaborations for Capacity Building

Karnataka Cyber Security Policy



Building Awareness

Skill Building

Promoting Research and Innovation

Promotion of Industry and Startups

Partnerships and Collaborations for Capacity Building

These pillars have been analysed through five distinct approaches:

(A) Whole-of-Government Approach: Cyber threats impact all segments of society. Building a strong cyber security ecosystem invariably will involve multiple departments of the State Government and several state government organisations. A holistic response system based on coordinated approaches between these entities is essential to building a strong cyber security ecosystem. Therefore, the Cyber Security Policy proposes a “Whole-of-Government” approach to ensure effective and efficient policy interventions, and to ensure synergy in the functioning of the government.

(B) Inclusive Policy Interventions: Cyberspace has emerged as a new but unequal domain where some groups are inherently disadvantaged. In keeping with the constitutional spirit of empowering the weaker sections to combat these inequalities, the Cyber Security Policy focuses on empowering vulnerable groups operating in cyberspace.

- Women face a disproportionate risk of cyberstalking, sexual harassment, matrimonial frauds and other gendered cybercrimes. This is further exacerbated due to their relatively lower awareness about state services, making women less able to defend themselves against these attacks.

- Youth and Children are increasingly using digital means for learning and entertainment. Additionally, a significant part of the social lives of youth and children occurs online, leaving them vulnerable to the attentions of ‘catfishers’ and other online predators. They should be sensitised about cyber security threats and common cyber-attacks and should be equipped to deal with them.

- Senior citizens, who may not be able to keep pace with the rapidly evolving nature of technology, are more vulnerable to cyber frauds and phishing attacks.

- Medium, Small and Micro Enterprises are in the process of digitizing their payment structures and operations, especially after the COVID-19 pandemic. However, they may not have the technical capacity and resources to adopt strong cyber risk mitigation strategies. Whilst adopting digital technologies widely is becoming an imperative to this sector, the lack of sufficient cyber risk management practices makes them more vulnerable to cyber threats.

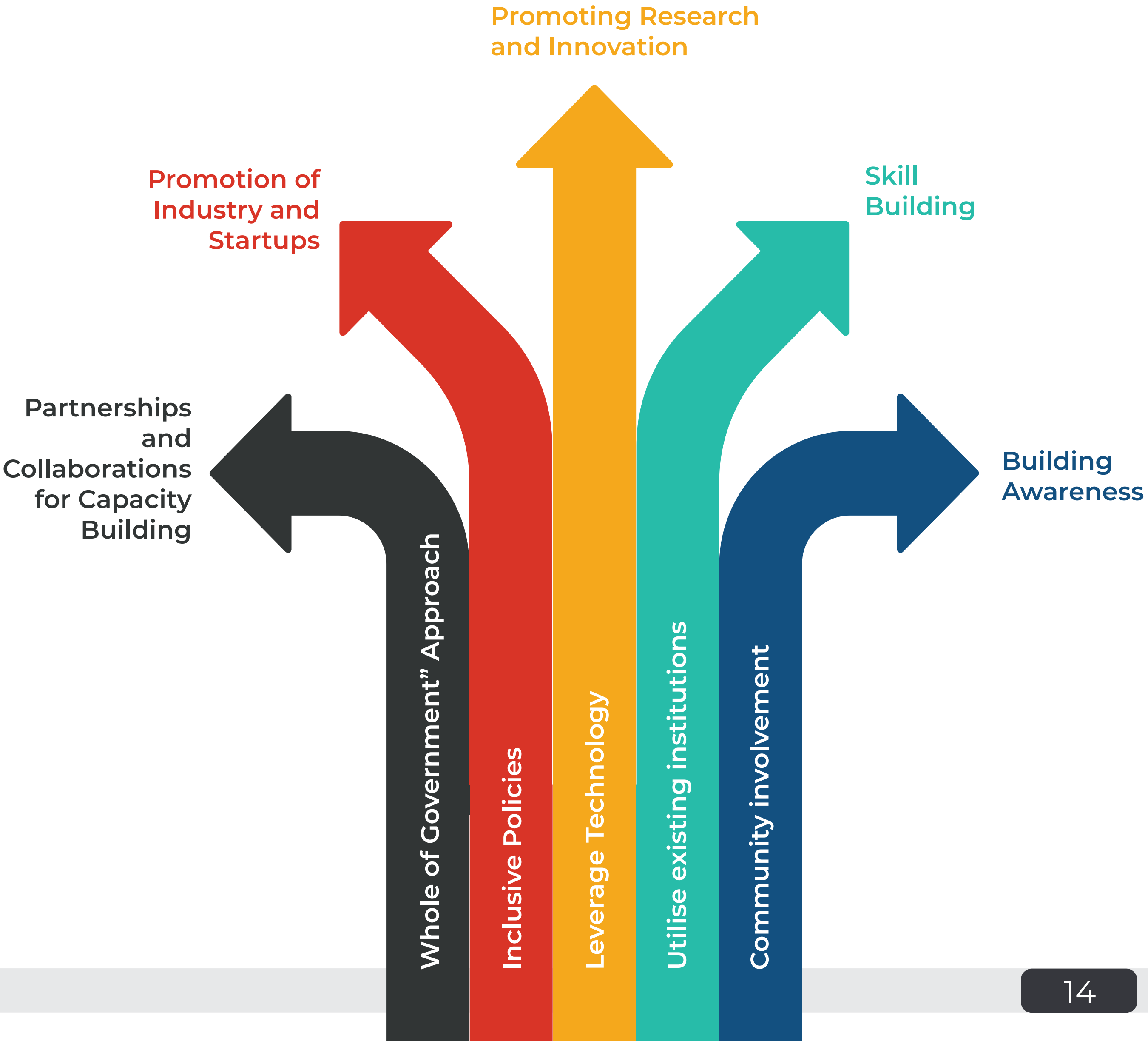
- First-Time Adopters of Online Technologies who are engaging with online spaces and devices such as smartphones for the first time. Such first-time adopters have only recently received internet connectivity and may need to be made aware of certain tenets of online hygiene. These citizens are particularly vulnerable to cyber frauds, lottery scams and banking frauds due to low digital literacy.

(C) Leveraging Technology: Leveraging technology is a critical aspect in solving the challenges in cyberspace and it is necessary to utilise the opportunities it provides. The Cyber Security Policy aims to leverage technology for ensuring efficiency, effectiveness and scale for achieving the agenda of the Policy.

(D) Leveraging the Existing Institutions & Policies: While cyberspace is nebulous and constantly changing, Government of Karnataka has been responding to these changes in the last three decades through various initiatives like Karnataka IT Policy, Karnataka Startup Policy and establishing a Centre of Excellence in Cyber Security. The efforts of these institutions and policies are synergised through this Cyber Security Policy to prevent duplication of efforts and optimise existing resources. This Cyber Security Policy, being a specialised document pertaining to the niche area of cyber security, develops from the concepts used in the broader policy documents for application in the field of cyber security.

(E) Community involvement: As a leading technology hub in the country, Karnataka is well placed to involve the technology community in building a strong cyber security ecosystem. This Cyber Security Policy will leverage the technology expertise in industry and academia, as well as the passion within the technology community for societal building, to foster partnerships.

The Policy strategy aims to address the cyber security challenges through the five pillars and lays down broad action points keeping in mind the approaches discussed in this section.


Promoting Research and Innovation
Promotion of Industry and Startups
Skill Building
Partnerships and Collaborations for Capacity Building
Building Awareness
Whole of Government" Approach
Inclusive Policies
Leverage Technology
Utilise existing institutions
Community involvement

PILLAR 1
BUILDING AWARENESS

Necessity for Policy Intervention

Cyber security awareness is a public good. Cyber-attacks and incidents of cyber-crime are rapidly growing and with the rapid adoption of the digital technologies by small businesses, thousands of citizens are now adopting unfamiliar technologies without being adequately equipped to safeguard their interest online. Similarly, these digitization processes have led to the generation of huge volumes of data. Awareness of data privacy and safe sharing and storage of data is the need of the hour. While national efforts to educate the public are ongoing, there is an increasing need for the State Government to undertake customised and targeted awareness campaigns that cater to the specific requirements of the citizens in Karnataka, especially in formats and languages most easily understood by them. Informed and knowledgeable citizens, being the first line of defence in a cyber-attack, are key pillars in achieving the objectives of this Cyber Security Policy and hence it is important for the state strategy to have a specific focus on it.

Policy Agenda

1.1 Regular cyber security and data privacy awareness sessions will be conducted, and best practices will be promoted, for all State Government departments, local bodies and panchayats. To ensure the effectiveness of the awareness programme, periodic assessments will also be conducted.

1.2 Cyber security awareness campaigns for public will be conducted regularly through various means, including social media and interactive technologies, and in partnership with industry and academia. This will also promote awareness and popularise the use of Dial 112 and Dial 1930 to report incidents of cyber-crime.

1.3 Easily accessible online awareness modules will be made available to the public and those completing various phases of assignments will be rewarded with certificates and encouraged to act as online volunteers to further the spread of awareness.

1.4 Awareness campaigns specifically tailored towards vulnerable sections such as women, youth and children, the elderly, start-ups and MSMEs transitioning into digital business modes and first-time adopters of online technologies, will be conducted.

1.5 Conduct surveys of the existing levels of cyber security and data privacy awareness amongst public in Karnataka and create a repository of related data, disaggregated by gender, education, and other social and economic indicators that will help identify gaps and target areas, including regional imbalances in awareness. The results of such surveys will be published.

1.6 Introduction of a basic awareness module on cyber security as part of college education to increase awareness amongst all future professionals about cyber safe practices while using digital technologies will be considered.

1.7 Awareness efforts will be decentralised by involving local educational institutions, local governance bodies and existing awareness schemes. A volunteer programme will be implemented to encourage the youth and other cyber aware citizens as peer educators and drivers of cultural change.

1.8 State Government led drives for adoption of technology such as the launch of new applications, online banking and digital literacy programmes will be accompanied by supporting cyber security awareness and training.

1.9 A repository of easily accessible online resources with links, including links to recognised international collections of spurious websites, helplines, fact-checking websites and other useful materials and informative resources will be created for citizens. This repository will also contain an explainer on the grievance redressal mechanisms available to citizens for various types of cyber-crimes and attacks.

1.10 The cyber security awareness programmes of various national agencies like Information Security Education and Awareness (ISEA) will be leveraged for the state programmes.

PILLAR 2
SKILL BUILDING

Necessity for Policy Intervention

There is a high demand for cyber security professionals in India and this demand is expected to grow exponentially in the coming years. Currently, despite the existence of isolated banks of expertise and training courses, there is an acute shortage of cyber security professionals in meeting the advancing needs of the digital economy. This is both a challenge and an opportunity. Karnataka, which is home to many prestigious technical institutes, is eminently placed to bridge this skills gap. Improved education avenues and skill development will further contribute to the achievement of other policy objectives like promoting the cyber security industry and strengthening state capacity.

Policy Agenda

2.1 Workshops will be conducted in colleges and universities in collaboration with local cyber security organisations and experts to raise awareness amongst the students regarding cyber security as a career option. These workshops will also create awareness regarding high-quality trainings and certifications available in the domain of cyber security.

2.2 The State Government will introduce a specialised course in higher education for students interested in cyber security specialisation within the framework of the New Education Policy, 2020.

2.3 Faculty Development Programmes will be run regularly in collaboration with industry experts to improve and update the skills of faculty in Higher Education Institutes.

2.4 Educational institutes will be encouraged and supported to prepare a cyber security policy that will address the cyber threats to their IT systems and define cyber risk management strategies.

2.5 A state-of-the-art virtual cyber range will be set up for strengthening practical skills amongst students of cyber security training programmes and to provide an experience of detection and mitigation of cyber-attacks in an interactive technology environment. Cyber range will also be utilised for training of Law Enforcement Agencies, prosecutors, government officials, judicial officers and cyber security related dispute mediators and conciliators.

2.6 Regional Centres of Excellence in cyber security will be established in a geographically distributed manner as multipurpose institutions for skill building activities. These regional Centres of Excellence will be utilised to enable awareness, research and for the assistance of government bodies facing cyber-attacks or responding to cyber-crimes. Physical cyber ranges and labs will be built in regional Centres of Excellence in partnership with industry for specialised cyber security training where physical access is necessary.

2.7 MOOCs (Massive Open Online Courses) in cyber security for interested citizens will be popularised with certification on completion.

2.8 Special emphasis will be placed on training women as cyber security professionals by offering subsidised training programmes for women, where subsidy is claimed in stages through the completion of the course.

2.9 A platform will be established to connect participants of specialised courses, training programmes and competitions with local start-ups and companies through internship programmes and recruitment drives.

2.10 Technical training in vocational training courses will be supplemented with training on secure practices that the technicians need to be aware of when implementing technology solutions.

PILLAR 3
PROMOTING RESEARCH AND INNOVATION

Necessity for Policy Intervention

Karnataka is the start-up capital of the country and a global innovation hub with more than 400 global R&D centres, ranking first in NITI Aayog's India Innovation Index with Bengaluru alone being the world's fourth largest technology and innovation cluster. The capital, infrastructure, talent and drive in the state present it with the unique opportunity to establish itself at the forefront of global R&D efforts in cyber security technology. In addition, there are many preferential areas of research that do not typically attract private capital and require state support for funding research into these areas in larger public interest.

Policy Agenda

3.1 Funding for research projects as mentioned in the Karnataka IT Policy will be extended for research projects in the domain of cyber security. Start-ups & MSMEs based in Karnataka, K-tech Innovation Hubs, centres of excellence and institutions with high National Institutional Ranking Framework (NIRF) and National Assessment and Accreditation Council (NAAC) ratings will be supported in cyber security research to ensure efficient utilisation of public monies with clear deliverables.

3.2 The triple helix model of innovation will be employed to foster development through collaboration between academia, industry, and government.

3.3 A "Use Case Clearing House" will be set up for identification of research problems for researchers /start-ups to convert into Proof of Concept (PoC).

3.4 In alignment with the Open Data Initiative, the State Government will pursue creating a culture of safe data sharing to improve quality of research. State Government departments, where possible, will encourage mutual collection, collation and sharing of cyber breach and vulnerability data between the government, law enforcement agencies and industry, including metadata, in sanitised formats. Such information sharing will provide early warning on cyber-attacks to other entities. The data will also be made available to select researchers and security service providers to aid research and analysis that can assist in building more relevant security solutions.

PILLAR 4
PROMOTION OF INDUSTRY AND START-UPS

Necessity for Policy Intervention

Karnataka has established its leadership position in the development of technological solutions. It is well positioned to drive indigenous efforts towards achieving the vision of self-reliance in critical technologies and cyber security solutions to meet the requirements of the country and export software products worldwide. To continue building Brand Karnataka, it is essential that the local cyber security industry and start-ups are encouraged to grow and thrive.

Policy Agenda

4.1 In synergy with the aims of the Karnataka Startup Policy, the State Government, through its incubation programmes, will identify promising start-ups in the cyber security space every year to receive specialised mentorship, intellectual property facilitation, and industry connect through partnerships.

4.2 Government will act as an early adopter and validator of cyber security solutions from start-ups where possible. Opportunities will be provided to select start-ups to conduct a proof of concept or pilot implementation with appropriate government entities.

4.3 Preferential procurement of cyber security solutions for government departments from Karnataka based start-ups, in line with the rules notified under Karnataka Transparency in Public Procurements Act, will be facilitated.

4.4 The State Government will reimburse the cost up to a maximum of INR 1 lakh towards engagement of Karnataka-based, CERT-In empanelled service providers by start-ups for cyber security audit, incident management and incident response activities. This may be availed by a start-up once over the period of this Cyber Security Policy.

4.5 Mentoring will be provided for business innovators in the state, in particular start-ups and MSMEs, to sensitise them to cyber risks and to instil a culture of "security by design" and "privacy by design".

4.6 The State Government will fund and support the building of testing infrastructure and facilities within Regional Centres of Excellence.

PILLAR 5
PARTNERSHIPS AND COLLABORATIONS FOR CAPACITY-BUILDING

Necessity for Policy Intervention

Increasingly sophisticated cyber-attacks and their widespread impact require coordinated and synchronised efforts across various segments of society. The expansive IT industry and infrastructure located in Karnataka necessitates the establishment of appropriate state level institutions to orchestrate such coordinated efforts. Further, government personnel, including law enforcement agencies should be equipped with skills commensurate with the challenges faced. Karnataka, as a visionary leader in technology, should take the lead in establishing apt procedures and capacity building measures related to cyber security, safety and privacy. Karnataka is also well-placed to leverage the technology depth available to meet such requirements.

Policy Agenda

5.1 A Cyber Security Steering Committee composed of representatives from key State Government departments, industry and academia will be constituted to guide the implementation of this Cyber Security Policy.

5.2 The state will establish K-CERT for effective coordination of responses to cyber security incidents at the state level. K-CERT will work under the guidance of CERT-In. The envisioned mandate of K-CERT will be three-fold:

- Advisory role for ensuring continuous desirable cyber security posture for government and industry
- Incident response and management for state government agencies, MSMEs and Start-ups
- Conduct security audits, including red-teaming exercises, for state government agencies, MSMEs and Start-ups

5.3 The K-tech Centre of Excellence in Cyber Security will be strengthened with cyber security experts, and leveraged for building required capacity building for government, industry and public at large. The CoE will support the government in defining and implementing secure software development processes. Cybercrime data available with Home Department will be shared with the CoE for dissemination of information to all stakeholders to prevent such attacks in future.

5.4 Regular technical and managerial training for state government officials will be conducted on cybersecurity best practices, cyber hygiene, and cyber risk management. Expertise from industry and academia will be leveraged for such trainings.

5.5 Publish appropriate cyber security standards for applicable suppliers and vendors of the state.

5.6 Develop a set of protocols for State Government officials to follow in online interactions and use of online resources, including email and social media, in their official capacity. All official email communications, whether internal or external, by State Government officials will be done exclusively through their official email IDs. The use of personal email IDs for such communication will be prohibited.

5.7 Select groups of adjudicators, mediators and conciliators will be specifically trained in appreciation of evidence and related aspects of cases of contravention of the IT Act. Centres of Excellence, cyber ranges and other training endeavours instituted under this Cyber Security Policy will be leveraged to train them.

5.8 The State Government will maintain a list of empanelled cyber security professionals who may act as amicus or advisors for specific cases as appropriate.

5.9 Partnerships with other cyber security hubs across India will be explored. Similarly, partnerships with cyber security hubs across the globe will be promoted through the Global Innovation Alliance programme.

5.10 All initiatives under this Cyber Security Policy are subject to the provisions of the National Cyber Security Policy as may be amended from time to time.

APPLICABILITY OF INCENTIVES

Policy Reference	Category	Incentive / Benefit
2.9	Internship	A stipend of Rs.10,000 per month will be provided, for maximum of 3 months, to Karnataka-based undergraduate interns who are doing internship related to cybersecurity. A stipend of Rs.15,000 per month will be provided, for maximum of 3 months, to Karnataka-based postgraduate interns who are doing internship related to cybersecurity. This will be provided to 200 undergraduate interns and 40 postgraduate interns in year 1 and year 2 of the policy applicability, with 400 undergraduate interns and 80 post graduate interns from year 3 onwards.
3.1	Research and Development	For R&D projects in the domain of cybersecurity, driven by Karnataka-based start-ups and in collaboration with Karnataka-based academic institutes, matching grant of up to a maximum of 50% of the total project R&D cost, or up to Rs. 50 lakhs, whichever is lower will be provided. These grants may be availed by an entity once over the policy period. Five such projects will be funded in each year.
4.4	Start-ups	Reimburse the cost up to a maximum of INR 1 lakh towards engagement of Karnataka-based, CERT-In empanelled service providers by start-ups registered with Karnataka Start-up Cell for cyber security audit, incident management and incident response activities. This may be availed by a start-up once over the policy period. This benefit will be provided to 100 start-ups each year.

VISION

> To build a dynamic, secure and resilient cyberspace for all the G2G, G2B and G2C services of Govt of Karnataka.

1. MISSION

01 To protect information and information assets of Govt of Karnataka from cyber threats.

02 To build capabilities and processes within the Government to prevent and respond to cyber threats effectively.

03 To proactively identify the vulnerabilities & cyber security risks associated with Information and Information systems of the Government and to take preventive action to minimize the damages from cyber incidents through a combination of Compliance to Cyber Security Standards and best practices, institutional structures, people, processes, technology and cooperation.

2. APPLICABILITY

01 This policy is in line with National Cyber Security Policy of India and applicable to all Government Departments and Government agencies of the state of Karnataka. It covers protection of information assets such as Hardware, System Software, Application Software, data, Databases, Network infrastructure and electronic Services of the Departments and agencies of the State Government.

02 This policy is applicable to private Agencies, third parties, contractors, outsourced partners, and personnel who are associated with departments and agencies of Karnataka Government in providing IT and IT enabled services.

03 This Policy applies to Central Infrastructure and Personnel who provide Services to the Karnataka Government either on specific deputation or by specific tasking.

04 Nothing in this Policy contravenes any applicable law of the Government of India or Government of Karnataka nor the policies of respective Governments. However, if any conflicts suspected, it must be brought to the notice of the Department of Personnel Administration and Reforms (e-Gov), Government of Karnataka immediately.

3. OBJECTIVES

01 To ensure secure delivery of all the electronic G2G, G2C and G2B services of Govt of Karnataka in cyberspace domain.

02 To build trust and confidence in the users in availing the government services through ICT platforms and thereby "encouraging" adoption of secured IT and ICT infrastructure in all the sectors of economy of the state.

03 To implement the Cyber Security Policy for Government of Karnataka., under the suitable framework for promotion and enabling actions for compliance towards the national and international standards & best practices

04 To closely work with the Law and Regulatory & Government agencies such as MeitY, CERT-In, NCIIPC, NCCC, Cyber Crime Wing of State Police etc., for security incident reporting and management.

05 To work with various OEMs/suppliers of Government departments and Government agencies to ensure adequate security controls have been built in the products, services & operations rendered by OEMs/suppliers for ensuring best adequate cyber security to the Government applications and Infrastructure. To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, that is consistent with industry standards.

06 To review and adopt to the latest threat management practice & principles and technology tools constantly towards achieving the maturity in cyber security management & operations and also to follow risk-based approach to for evaluating security controls.

07 To encourage the wider usage of IT/ICT infrastructure by all the departments of Government for trusted communication, transactions and authentication.

08 To establish Security Operation Centre (SOC) for all the Government critical IT Infrastructure projects for obtaining strategic information regarding incidents, threats reported as part of the Infrastructure and its system by creating incident response, crisis management through effective, predictive, preventive, protective, response and recovery actions on24/7 basis.

09 To deal with any cyber crisis effectively, through the process, a cyber crisis management plan will be drafted and implemented

10 To support capacity building activities by enabling Awareness & Training activities to the Government staff and to promote cyber security culture.

11 To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing damages/losses due to cybercrime or data theft.

12 To transfer cyber risks associated with cyber threats upon the assessment to the cyber insurance providers through Cyber insurance & Cyber Crime policy.

13 To enable effective prevention, investigation and prosecution of cyber-crime and enhancement of law enforcement capabilities.

14 To create skilled staff workforce in cyber security across the Government departments and Government agencies through capacity building, skill development and training.

15 To encourage Government departments and Government agencies to set aside financial provision for continually evaluate the cyber risks & to take appropriate measure to contain those risk includes strengthening cyber security of their ICT infrastructure, information and information processing assets.

16 To conduct periodic audit of IT infrastructure and applications of the departments by CeG to assess compliance to the cyber security controls and to prevent cyber-attacks. CeG to build required team and also engage CERT-in empanelled agencies to conduct the audits.

4. CYBER SECURITY ARCHITECTURE FRAMEWORK OF KARNATAKA

The Cyber Security Architecture Framework of Karnataka (CSAF-KA) defines the overall ambit of the Cyber Security related Agencies in Karnataka. The Cyber Security Architecture of Karnataka (CSAF-KA) will be executed by DPAR (e-Governance). The major components that constitute the CSAF-KA are :

(a) Legal & Regulatory Framework
(b) Compliance and Enforcement Framework
(c) Capacity Building and Cyber security Culture Framework
(d) Collaboration Framework

The Cyber security Policy Framework holds several other frameworks that are intended to provide a holistic and complete solution the cyber security threat. The four pillars that hold up the State VISION cyber security policy framework are as under:

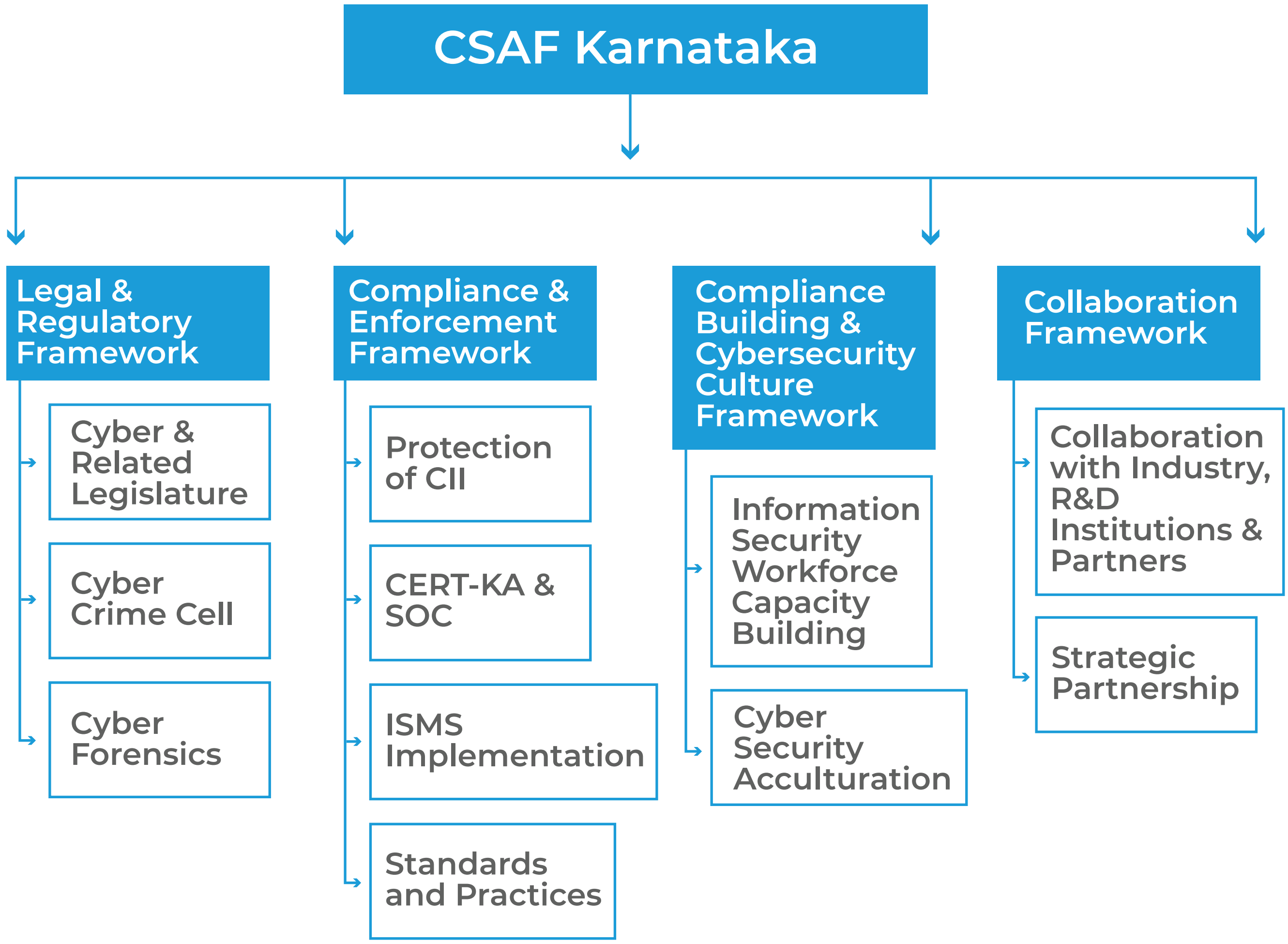
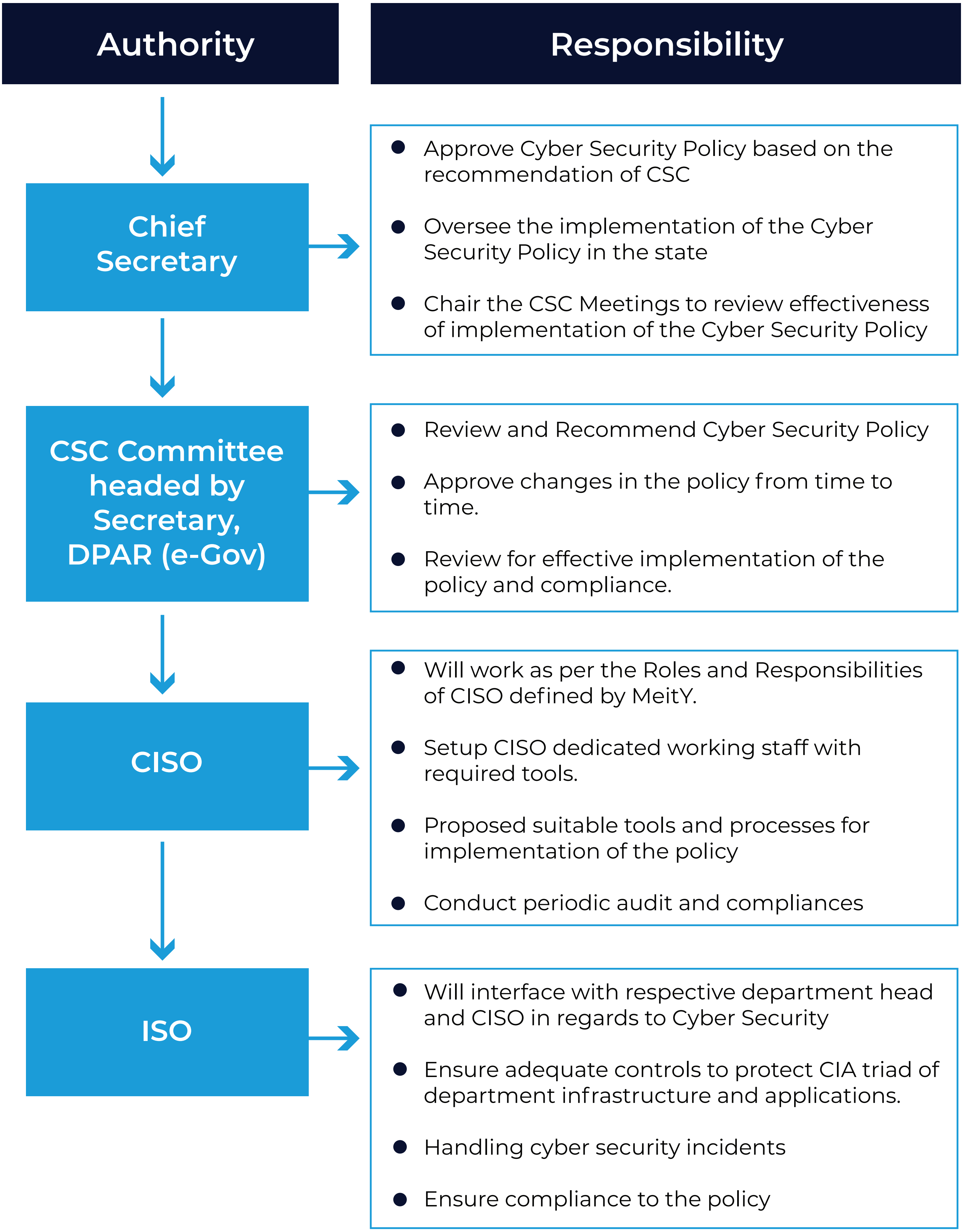

CSAF Karnataka
Legal & Regulatory Framework
Cyber & Related Legislature
Cyber Crime Cell
Cyber Forensics
Compliance & Enforcement Framework
Protection of CII
CERT-KA & SOC
ISMS Implementation
Standards and Practices
Compliance Building & Cybersecurity Culture Framework
Information Security Workforce Capacity Building
Cyber Security Acculturation
Collaboration Framework
Collaboration with Industry, R&D Institutions & Partners
Strategic Partnership

FIGURE 1: CYBER SECURITY ARCHITECTURE FRAMEWORK COMPOSITION.

The Architecture is an overall framework composition that allows Government Departments to access centralized resources, Compliance, Incident Handling Assistance and Monitoring without hindering their unfettered ownership and handling of their resources., Several aspects of the Architecture will be dynamic in adapting to technological changes.

5. CYBER SECURITY GOVERNANCE STRUCTURE



Authority | **Responsibility**

Chief Secretary

- Approve Cyber Security Policy based on the recommendation of CSC
- Oversee the implementation of the Cyber Security Policy in the state
- Chair the CSC Meetings to review effectiveness of implementation of the Cyber Security Policy

CSC Committee headed by Secretary, DPAR (e-Gov)

- Review and Recommend Cyber Security Policy
- Approve changes in the policy from time to time.
- Review for effective implementation of the policy and compliance.

CISO

- Will work as per the Roles and Responsibilities of CISO defined by MeitY.
- Setup CISO dedicated working staff with required tools.
- Proposed suitable tools and processes for implementation of the policy
- Conduct periodic audit and compliances

ISO

- Will interface with respective department head and CISO in regards to Cyber Security
- Ensure adequate controls to protect CIA triad of department infrastructure and applications.
- Handling cyber security incidents
- Ensure compliance to the policy

5.1 CHIEF SECRETARY, GOVERNMENT OF KARNATAKA

- Approval the Cyber Security Policy based on the recommendation of the CSC
- Oversee the implementation of the Cyber Security Policy in the state.
- Chair the CSC meetings to review the implementation, periodic audits for compliance, continual improvements in strengthening cyber security for the state.

5.2 COMPOSITION AND ROLES OF CYBER SECURITY COMMITTEE (CSC)

CSC shall have following members

- Additional Chief Secretary (ACS)/ Pr. Secretary/Secretary-DPAR (e-Governance).
- Additional Chief Secretary (ACS)/ Pr.Secretary/Secretary-Dept of IT, BT & ST.
- Chief Executive Officer, CeG.
- CISO for Karnataka State.
- Information Security Officers of Dept of Finance, Law, Revenue, Home, Health, Education, Energy, UDD, BBMP and Other relevant Govt agencies.
- Representatives from CDAC, IISc, NLSIU & IIIT-Bangalore.
- Any other technical offices deemed fit by CISO.

Roles of CSC

- Review the Cyber Security policy and recommend for approval.
- Conducting periodic meeting to identify risks associated with IT infrastructure and applications of the state and mechanism to deal with mitigating the risks.
- Setting up incident management response plan for the state.
- Recommend for funding for effective implementation of cyber security policy.
- Approve all policy matters related to Information Security and changes thereto.
- Approve exceptions on a case-by-case basis when the requirements of the Cyber Security policy cannot be met, provide a timeline for the exception and follow-up the exception condition till the Security Policy requirements are met.
- Review status of Cyber Security implementations and Audits.
- Review of the compliance to the relevant laws including IT Act and also provide inputs to formulation of state legal frameworks for cyber security.
- Formulating Cyber Crisis Management Plan.
- Overseeing the DR/BCP operations.
- Empowering the CISO to take necessary actions to strengthen the cyber security in the state and policy deviations reported/noticed.

5.3 HEAD OF THE DEPARTMENTS

01 Hold the primary responsibility for enforcing this policy and defining the values and classification of assets within their control by participating in the risk management process and undertaking business impact assessment.

02 Authorizing and approving access for the concerned stakeholders including designing and maintaining segregation of duties for stakeholder group/ individual users and groups including third party agency to the information possessed by the Department's applications and support Infrastructure.

03 Ensure implementation and compliance to IT Act, Cyber Security policy and relevant laws as applicable.

04 Carry out periodic IT security risk assessments and determine acceptable level of risks, consistent with criticality of business/functional requirements, likely impact on business/functions and achievement of organisational goals/objectives. Nominating head of the e-Gov cell or Head of IT division of the respective department as Information Security Officer (ISOs).

5.4 CHIEF INFORMATION SECURITY OFFICER (CISO)

01 Will work as per the roles and responsibilities defined by MeitY, Govt of India including amendments issued from time to time.

02 Setup its own dedicated team of experts (Cyber Security Expert, Application and Network Expert, Co-ordinators, Legal Expert).

03 Evaluate and recommend suitable strategic infrastructure, security tools and processes to enhance the security posture of the state's ICT infrastructure and applications.

04 Establish and maintain a cyber risk register.

05 Compliance to IT Act and its amendments from time to time.

5.5 INFORMATION SECURITY OFFICERS (ISOs) OF DEPARTMENTS

01 Shall interface with state CISO and /Departments in relation to information / cyber security related issues and bring the cyber security culture in its organization by conducting awareness programmes, trainings etc.

02 Co-ordinating and reporting to State CISO in regards to fixing the vulnerabilities if any as reported from NCIIPC, NCCC and CERT-In etc from time to time.

03 Should ensure that department's IT/ICT Infrastructure shall comply with the cyber security policy on an ongoing basis (Regular patch updates, firmware updates, role-based access to the systems/applications, review of password change policy, Email security, data security, data leakage prevention modes, applicability of controls at all the appropriate levels etc).

04 Ensuring the implementation of Karnataka cyber Security policy and its Standards across the ICT infrastructure & applications of the concerned department.

05 Provide guidance to concerned stake holders for implementation of security policies and standards.

06 Monitor the security related activities carried out by concerned stake holders (applications providers, infra providers, vendors, maintenance agencies etc).

07 Monitor and assess the compliance to security policies, procedures and standards on an ongoing basis and report exceptions to CISO.

08 To authorize to perform periodic information security audits, Risk Assessment & Treatment and Web Application Security Assessment (WASA) & Vulnerability Assessment and Penetration Testing (VAPT) for the applications.

09 Provide Cyber Security requirements and inputs to CISO.

10 Obtain approval of CSC for exception if any.

11 Administer the security awareness program among the employees.

12 Act as point of contact for their respective department for Cyber Security policies, issues and concerns.

13 Facilitate the resolution of security conflicts within the organization and escalation of the same to the CISO.

14 Ensure Incident Management including Incident Response is carried out efficiently as per CERT-in Directives dated 28th April 2022.

15 Conduct regular and spot audits to determine compliance to Cyber Security policy.

16 Developing contingency plans for Disaster Recovery/Business Continuity Planning for the departmental applications and formulate Cyber Crisis Management Plan for the department.

17 Compliance to IT Act and its amendments from time to time.

6. STRATEGIES

A. CREATING A SECURE CYBER ECOSYSTEM

The cyber security ecosystem revolves around the core values of the state's data, information and information system and all the state's ICT infrastructure to continuously protect them from cyber threats. The ecosystem consisting of all the departments and government agencies of the state, Governance Structure, CISO, ISOs, Legal and Partnership, OEM/Suppliers, APT teams, auditors etc.

01 To coordinate all matters related to cyber security in the state, with clearly defined roles & responsibilities by the nodal agency DPAR- e-Governance.

02 To encourage all the departments to designate a member of senior management, as Information Security Officer (ISO), responsible for cyber security efforts and initiatives. The Key Roles and Responsibilities of ISO will be as defined in this policy.

03 To encourage all the government departments to implement this policy aligning to department's functions and requirements and also implement industries best practices. Establishing standards and mechanisms for secure information flow (while in process, handling, storage & transit), crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

04 To ensure that all the departments and agencies earmark a specific budget for implementing cyber security initiatives and for meeting emergency response arising out of cyber incidents.

05 To prevent occurrence and recurrence of cyber incidents by way of incentives for technology development, cyber security compliance and proactive actions.

06 To establish a mechanism for sharing information and for identifying and responding to cyber security incidents and for cooperation in restoration efforts.

07 To encourage entities to adopt guidelines for procurement of trustworthy ICT products and provide for procurement of indigenously manufactured ICT products that have security implication.

B. CREATING AN ASSURANCE FRAMEWORK

The objective of this strategy is to design an outline in compliance with the global security standards through traditional products, processes, people, and technology.

01 To promote adoption below of global best practices in information security and compliance and thereby enhance cyber security posture.

- Inventory all IT assets.
- Define a secure software development methodology.
- Prepare a reference security architecture that can be leveraged by other teams and projects.
- Conduct a security assessment.
- Prioritize cybersecurity risks.
- Monitor critical security vulnerabilities.
- Develop an incident management plan.
- Automate threat detection, remediation, and mitigation.
- Transition to a DevSecOps policy.
- Consider cybersecurity training.

02 To create & maintain infrastructure for conformity assessment and certification of compliance to cyber security best practices, standards and guidelines (E.g. ISO 27001 ISMS certification, IS system audits, Penetration testing / Vulnerability assessment, application security testing, web security testing).

03 To enable implementation of global security best practices in formal risk assessment and risk management processes, business continuity management and cyber crisis management plan by all entities within Government and in critical sectors, to reduce the risk of disruption and improve the security posture.

04 To identify and classify information infrastructure facilities and assets at entity level with respect to risk perception for undertaking commensurate security protection measures.

05 To encourage secure application / software development processes based on global best practices.

06 To create conformity assessment framework for periodic verification of compliance to best practices, standards and guidelines on cyber security.

07 To encourage all entities to periodically test and evaluate the adequacy and effectiveness of technical and operational security control measures implemented in IT systems and in networks.

C. STRENGTHENING LEGAL AND REGULATORY FRAMEWORK

01 To adopt to the legal framework including IT Act and rules/notifications.

02 To mandate periodic audit and evaluation of the adequacy and effectiveness of security of information infrastructure as may be appropriate to ensure compliance with respect to regulatory framework.

03 To create awareness to enable, educate and facilitate awareness of the regulatory framework.

D. CREATING MECHANISM FOR INCIDENCE HANDLING, VULNERABILITY MANAGEMENT AND RESPONSE TO SECURITY THREATS

01 To create State level systems, processes, structures and mechanisms to generate necessary situational scenario of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.

02 To work closely with National Level Computer Emergency Response Team (CERT-In), the Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management in the country.

03 To operationalise Security Operations Centre (SOC) for all coordination and communication actions within the respective departments for effective incidence response & resolution and cyber crisis management of the state's common ICT infrastructure.

04 To develop and implement Cyber Crisis Management Plan for dealing with cyber related incidents impacting critical state's processes or endangering public safety and security of the state by way of well-coordinated, multi-disciplinary approach at the State, Sectoral as well as entity levels.

05 To conduct and facilitate regular cyber security drills & exercises at government departments, and government agencies to enable assessment of the security posture and level of emergency preparedness in resisting and dealing with cyber security incident.

06 To define data retention policy based on the type and criticality of data to ensure high availability and log retention policy to support any investigations of data breach.

07 Reporting cyber security incidents as listed under Annexure-1 of CERT-In Directives under sub-section 6 of 70(B) of IT Act.

E. SECURING E-GOVERNANCE SERVICES

01 To mandate implementation of global security best practices, business continuity management and cyber crisis management plan for all e-Governance initiatives in the state, to reduce the risk of disruption and improve the security posture.

02 To ensure security for E-Governance applications of various departments with regards to the data and privacy protection through the following measures:

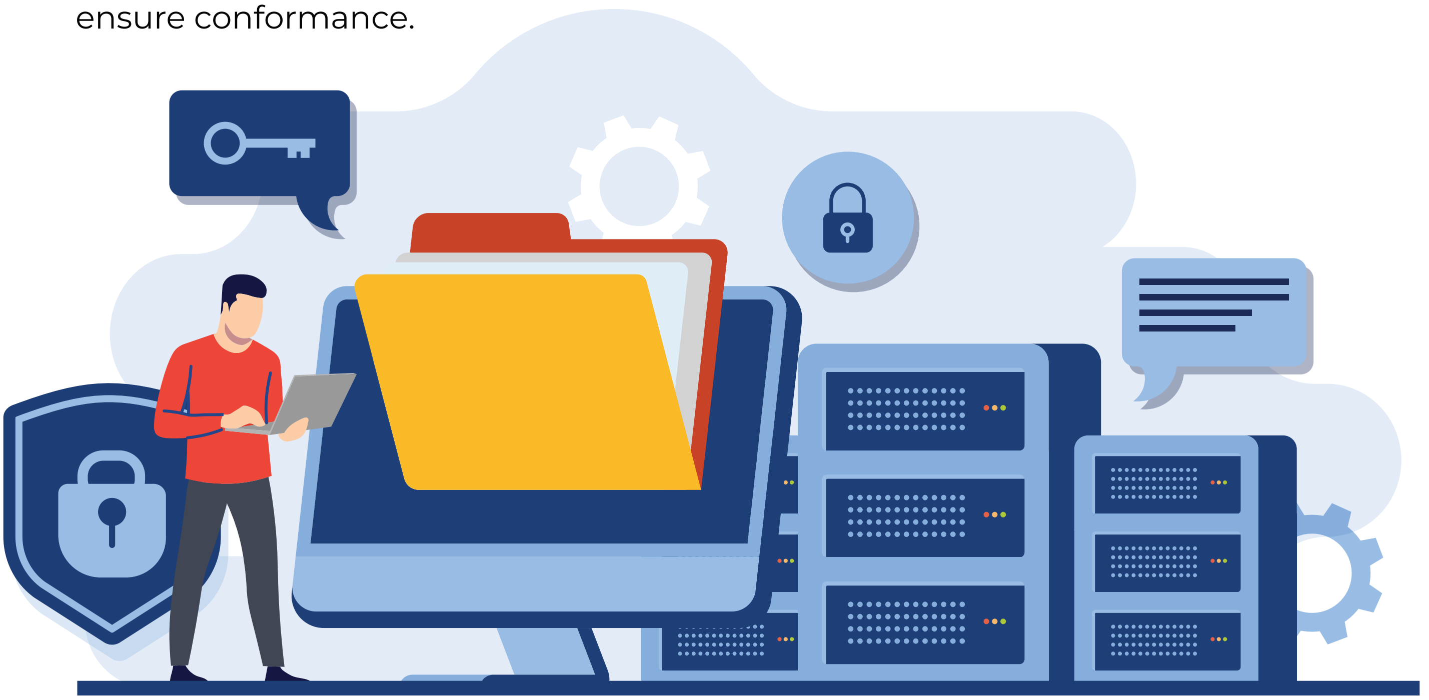
- Network security (NIPS, Firewalls, content filtering, HIPS, antivirus, etc.).
- Data security (at rest, in transmit, in process and in use by deployment for various tools and technologies with linked to the processes).
- Application security (audited by CERT-In empanelled TPA).
- DR/BCP provisioning (real-time data is replicated to DR site in case of any physical calamity or damage to resources at primary site, backup exists at remote different seismological locations).
- Application and Data back-up as per department's backup policy & requirement.
- Have multi-factor authentication with Identify & Access Management for IT infrastructure and applications.

03 To encourage wider usage of Public Key Infrastructure (PKI) within Government for trusted communication and transactions.

04 To adopt to MeitY's Cloud Security best practices for availing cloud services from the MeitY empanelled Cloud Service Providers.

05 To enforce information classification across all processes, functions and operations of the departments. To have adequate controls in place for safeguarding PII data.

06 To engage experts from the field including information security professionals / organisations and experts from academia to assist e-Governance initiatives and ensure conformance.



F. RISK ASSESSMENT, RISK TREATMENT PLANS

01 Define a Security Risk Assessment (SRA) process to ensure periodic assessment of all IT systems (applications, infrastructure components, endpoints, peripheral IT devices, etc). Unlike an audit, SRA will be a forward-looking assessment that will review the threats to the IT system and provide recommendations to treat the risk.

02 Conduct regular security risk assessments of the state's IT systems as defined in the process.

03 Prepare and maintain an organisational security risk register that will be a collation of the cyber risks identified from various sources. This consolidated risk register will provide a view of the cyber risk profile across various dimensions.

04 To encourage all the departments to conduct Risk Assessment for their respective Information and Information assets and have appropriate risk treatment plans as per ISO 27001.

05 To explore the option of transferring the cyber risks associated with critical ICT infrastructure to the cyber insurance providers by way of procuring cyber risk and cybercrime insurance policies from the IRDAI registered entities.

G. PROTECTION AND RESILIENCE OF CRITICAL INFORMATION INFRASTRUCTURE.

01 To develop a plan for protection of Critical Information Infrastructure and its integration with business plan at the entity level and implement such plan. The plans shall include establishing mechanisms for secure information flow (while in process, handling, storage & transit), guidelines and standards, crisis management plan, proactive security posture assessment and forensically enabled information infrastructure.

02 To work closely with National Critical Information Infrastructure Protection Centre (NCIIPC), the nodal agency for critical information infrastructure protection in the country.

03 To facilitate identification, prioritisation, assessment, remediation and protection of critical infrastructure and key resources based on the plan for protection of critical information infrastructure as laid down by NCIIPC.

04 To mandate implementation of global security best practices, business continuity management and cyber crisis management plan by all critical government entities, to reduce the risk of disruption and improve the security posture.

05 To encourage and mandate as appropriate, the use of validated and certified IT products.

06 To mandate security audit of critical information infrastructure on a periodic basis.

07 To mandate certification for all security roles right from CISO / CSO to those involved in operation of critical information infrastructure.

08 To mandate secure application / software development process (from design through retirement) based on global best practices.

09 To mandate hosting only the security complied applications at the state data centre.

10 To mandate periodic VAPT & WASA of the common ICT infrastructure and government applications, mobile applications and APIs through CERT-In empanelled agencies.

H. REDUCING SUPPLY CHAIN RISKS.

01 To evaluate the products/solutions for its compliance as per global standards and practices before adopting them in the critical production environments by way of enforcing the mandatory tests on the hardware and software in the staging environment before they would be put into production.

02 To build trusted relationships with product / system vendors and service providers for improving end-to-end supply chain security visibility and mandating that OEM to undertake that the supplied products are free from such cyber threats in the entire supply chain.

03 To create awareness of the threats, vulnerabilities and consequences of breach of security among government departments & agencies for managing supply chain risks related to IT (products, systems or services) procurement

I. HUMAN RESOURCE DEVELOPMENT AND CYBER SECURITY AWARENESS

01 To foster education and training programs for government staff to support national as well as state's cyber security needs and build capacity.

02 To work closely with Cyber security training agencies, legal experts, academia identified by the state to promote awareness and trainings to the staff.

03 To support institutional mechanism for capacity building for Law Enforcement Agencies To conduct, support and enable cyber laws and cyber security workshops/seminars and certification programs for government staff.

04 To promote the cyber security culture among the government staff.

J. COLLABORATION & PARTNERSHIPS

01 To facilitate collaboration and cooperation among stakeholder entities including private sector, in the area of cyber security in general and protection of critical information infrastructure in particular for actions related to cyber threats, vulnerabilities, breaches, potential protective measures, and adoption of best practices.

02 To create models for collaborations and engagement with all relevant stakeholders such as NCIIPC, CERT-in, Cyber Swatchta Kendra, NCCC, C&IS Division of MHA, IIIT-B, IISc and Cyber Security OEMs, to strengthen government information and information systems.

03 To create an apex cyber security committee including external experts for cyber security policy inputs, discussion and deliberations.

K. USAGE OF IT RESOURCES OF GOVT OF KARNATAKA & COMPLIANCE

01 To comply with MeitY's policies on the usage of IT resources for Govt.Departments and Govt organizations which covers Network Access Policy, Computer usage policy, e-mail policy, Bring Your Own Device (BYOD) Policy etc published periodically.

02 To enforce security policy onto the IT systems/devices provided by the government to the staff of all the departments.

03 To review the policy implementation periodically and enforcing appropriate action for deviations to mitigate the chances of cyber threats.

MeitY's Policy on usage of IT resources of GoI -2014

L. SOCIAL MEDIA POLICY

01 To sensitive the government staff on the usage of social media in the government communication and to ensure data protection, security, privacy, archiving etc.

02 To promote best practices as regards to the use of social media as per the Government of India's Framework and Guidelines of for the use of social media for government organisations.

M. CHANGE MANAGEMENT

All the changes/upgrades to the ICT infrastructure and applications should undergo the change management process of change initiation, validation and approval. A centralised change control board under CeG will be setup to review the changes and accord approvals.

N. REVIEW OF POLICY

To review the policy by the committee under the chairmanship of Secretory, DPAR (e-Governance) at least once in two years for adapting to the best practices/processes and to keep the policy updated &dynamic to address the changing cyber threat landscape.

O. PRIORITIZED APPROACH FOR IMPLEMENTATION

To adopt a prioritized approach to implement the policy so as to address the most critical areas in the first instance.

P. OPERATIONALIZATION OF THE POLICY

01 This policy shall be operationalised by way of detailed guidelines and plans of action at various levels of the government departments as may be appropriate, to address the challenging requirements of security of the cyberspace.

02 The mapping of the policy objective to the proposed strategies is given in the Annexure A.

Annexure A :

Mapping of Karnataka State Cyber security policy objectives with Strategies

Sl. No	Objectives	Strategy as proposed in policy
01	To ensure secure delivery of all the electronic G2G, G2C and G2B services of Govt of Karnataka in cyberspace domain.	Creating a secure cyber ecosystem and Securing e-Governance Services
02	To build trust and confidence in the users in availing the government services through ICT platforms and thereby "encouraging" adoption of secured IT and ICT infrastructure in all the sectors of economy of the state.	● Protection and Resilience of Critical Information ● Infrastructure and Securing e-Governance Services
03	To implement the Cyber Security Policy for Government of Karnataka., under the suitable framework for promotion and enabling actions for compliance towards the national and international standards & best practices	● Creating an assurance framework ● To create & maintain infrastructure for conformity ● Strengthening Legal and Regulatory framework
04	To closely work with the Law and Regulatory & Government agencies such as MeitY, CERT-In, NCIIPC, NCCC, Cyber crime-police etc., for security incident reporting and management.	Collaboration & Partnerships
05	To work with various OEMs/suppliers of Government departments and Government agencies to ensure adequate security controls have been built in the products, services & operations rendered by OEMs/suppliers for ensuring best adequate cyber security to the Government applications and Infrastructure. To encourage the adoption of information security best practices by all entities and Stakeholders in the Government, that is consistent with industry standards.	Reducing Supply Chain Risks and Usage of IT resources of Govt of Karnataka & Compliance

Sl. No	Objectives	Strategy as proposed in policy
06	To review and adopt to the latest threat management practice & principles and technology tools constantly towards achieving the maturity in cyber security management & operations and also to follow risk-based approach to for evaluating security controls	Creating Mechanism for Incidence Handling, Vulnerability Management and Response to Security Threats
07	To encourage the wider usage of IT/ICT infrastructure by all the departments of Government for trusted communication, transactions and authentication.	● Securing e-Governance Services. ● Risk Assessment, Risk Treatment Plans.
08	To establish Security Operation Centre (SOC) for all the Government critical IT Infrastructure projects for obtaining strategic information regarding incidents, threats reported as part of the Infrastructure and its system by creating incident response, crisis management through effective, predictive, preventive, protective, response and recovery actions on 24/7 basis.	To operationalise Security Operations Centre (SOC).
09	To deal with any cyber crisis effectively, through the process, a cyber crisis management plan will be drafted and implemented.	● To conduct and facilitate regular cyber security drills security incident. ● To work closely with National Level Computer Emergency Response Team (CERT-In), the Nodal Agency for coordination of all efforts for cyber security emergency response and crisis management in the country.
10	To support capacity building activities by enabling Awareness & Training activities to the Government staff and to promote cyber security culture.	Human Resource Development and Cyber Security Awareness

Sl. No	Objectives	Strategy as proposed in policy
11	To enable protection of information while in process, handling, storage and transit so as to safeguard privacy of citizen's data and reducing damages/losses due to cybercrime or data theft.	Collaboration & Partnerships
12	To transfer cyber risks associated with cyber threats upon the assessment to the cyber insurance providers through Cyber insurance &/or Cyber Crime policy.	Risk Assessment, Risk Treatment Plans
13	To enable effective prevention, investigation and prosecution of cyber-crime and enhancement of law enforcement capabilities.	Projection and Resilience of Critical Information Infrastructure
14	To create skilled staff workforce in cyber security across the Government departments and Government agencies through capacity building, skill development and training.	Human Resource Development and Cyber Security Awareness
15	To encourage Government departments and Government agencies to set aside financial provision for continually evaluate the cyber risks & to take appropriate measure to contain those risk includes strengthening cyber security of their ICT infrastructure, information and information processing assets.	Collaboration & Partnerships
16	To conduct periodic audit of IT infrastructure and applications of the departments by CeG to assess compliance to the cyber security controls and to prevent cyber-attacks. CeG to build required team and also engage CERT-in empanelled agencies to conduct the audits.	● Creating an assurance framework ● Strengthening Legal and Regulatory framework ● Securing e-Governance Services ● Risk Assessment and Risk Treatment

REFERENCES

- Digital India: Technology to transform a connected nation', McKinsey Global Institute (March 2019); 'Internet Adoption in India: ICUBE 2020', IAMAI and Kantar (June 2021); Asli Demirguc-Kunt et al., 'The Global Findex database 2017: measuring financial inclusion and the Fintech revolution', World Bank (April 2018).
- National Cyber Security Policy 2013 – MeitY
- Cloud Security Best Practices of MeitY
- CERT-In Directives dated 28th April 2022
- 'Global Risks Report', World Economic Forum (2020).
- 'Internet Security Threat Report', Volume 24, Symantec (February 2019).
- 'Karnataka Cyber Security Vision, 2025', Karnataka Jnana Yoga (2019).
- Cyber Crimes against Women - 2020, Crime in India 2020, Volume I, National Crime Records Bureau.
- National Family health Survey – 5, Karnataka State Report; Giorgia Barboni, Erica Field, Rohini Pande, Natalia Rigol, Simone Schaner, Charity Troyer Moore, 'A Tough Call: Understanding barriers to and impacts of women's mobile phone adoption in India', Harvard Kennedy School (October 2018); 'Bridging the Digital Divide for Girls in India', Digital Empowerment Foundation and Centre for Catalyzing Change (2020).
- A Handbook for Adolescents/Students on Cyber Safety, Ministry of Home Affairs; Dr. Nagarathna A, Jay Bhaskar Sharma and Sparsh Sharma, 'Children and Cyber Safety – an e-Book', Advanced Centre For Research, Development And Training In Cyber Laws And Forensics, NLSIU, Bangalore; 'Child Online Protection in India', UNICEF (2016).
- Kartikeya Tripathi, Sarah Robertson and Claudia Cooper, 'A brief report on older people's experience of cybercrime victimization in Mumbai, India', Journal of Elder Abuse & Neglect, Volume 32 Issue 4 (2019).
- Report on Incentivizing Responsible and Secure Innovation', World Economic Forum (2020).
- 'Global Risks Report', World Economic Forum (2020); 'Internet Security Threat Report', Volume 24, Symantec (February 2019).
- 'Cyber Security India Market - What lies beneath', Price Waterhouse Coopers (2019).
- 'State of Cybersecurity in India', Analytics India Magazine and Jigsaw Academy (2020); 'Future Series: Cybersecurity, emerging technology and systemic risk - Insight Report', World Economic Forum and University of Oxford (November 2020).

R
C
mp3
T

Managing Director

Karnataka Innovation and Technology Society
BMTC Building 4th Floor (TTMC ‘B’ Block-above
Bus Stand) Shanti Nagar, Bengaluru – 560027, India

Tel	**:**	+91-80-22231006
Telefax	**:**	+91-80-22727480
E-mail	**:**	kitsgok@karnataka.gov.in md.ktech@karnataka.gov.in
Visit	**:**	itbtst.karnataka.gov.in